REMARKS/ARGUMENTS

This Amendment is in response to an Office Action mailed August 27, 2004. In the Office Action, claim 28 was rejected under 35 U.S.C. §112, first paragraph and claims 1-28 were rejected under 35 U.S.C. §103(a). Applicant respectfully traverses these rejections.

Rejection Under 35 U.S.C. §112

Claim 28 was rejected under 35 U.S.C. §112, first paragraph. Applicant has amended claim 28 to overcome the rejection. Withdrawal of the rejection is respectfully requested.

Rejection Under 35 U.S.C. §103

Claims 1-28 were rejected under 35 U.S.C. §103(a). Applicant respectfully traverses the rejections and contends that a *prima facie* case of obviousness has not been established for each of the pending claims. In the event that the pending claims are not considered by the Examiner to be in allowable condition, Applicant respectfully requests the Examiner to identify which items of the cited references are equivalent to the limitations set forth in the claims. This listing would facilitate prosecution of the subject application

For instance, claim 1 is rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier ("Applied Cryptography") in view of Menezes §12.3 ("Handbook of Applied Cryptography," section 12.3). Applicant respectfully traverses the rejection and contends that upon *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See MPEP §2143, p. 2100-124 (8th Ed., rev. 1, Feb. 2003); See also In re Fine*, 873 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988). Herein, at a minimum, the combined teachings of the cited references do not describe or suggest all of the claim limitations.

As an example, in contrast with the contention set forth in paragraph 6 of the Office Action, Applicant respectfully submits that both Schneier and Menezes §12.3 fail to disclose or even suggest that the data is stored in a protected area of internal memory of the first device *that prevents subsequent modification of the data.* Emphasis added.

Moreover, Schneier and Menezes §12.3 fail to disclose or suggest generation of a secret value within the first device where the secret value is a combination of both (1) data stored in protected area of internal memory of the first device that prevents subsequent modification of the data and (2) a short term value generated *in response to a periodic event being a power-up cycle.* Emphasis added.

For instance, on page 499 of Menezes §12.3, the authenticated key exchange protocol identifies that entities A and B share long-term symmetric keys (K, K'). The session key (W), considered to be the secret value as claimed, is derived based on either a Medium Access Control "MAC" value (h_K) or a pseudo-random permutation (or keyed one way function) performed on a random number produced at entry B (h_K). The B entity is considered to be the "second" device, separate and apart from the first device as claimed. The authenticated key exchange protocol of Menezes §12.3 fails does not involve a production of the secret value (session key "W") based on the long-term data and the short term value produced internally within the first device *at every power-up cycle*. Emphasis added.

In fact, consistent with this analysis, the Examiner has stated that neither Schneier nor Menezes §12.3 discloses a periodic event including a power up sequence. The intrinsic properties of volatile memory, namely the loss of data at power-down which would require reloading of data (e.g., short term value), does not suggest generation of the short term value (data) at every power-up cycle for combination with the long term value as set forth in amended claim 3. As aptly stated by the Federal Circuit, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *See In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). Here, it is not the case.

In view of the foregoing, Applicant respectfully requests withdrawal of the §103(a) rejection as applied to new independent claim 3 and those claims dependent thereon.

Claims 2-7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Menezes §12.3 and Ugon (USP 4,795,893). Applicant respectfully traverses this rejection in its entirety. The grounds for traverse of claim 3 are set forth above. With respect to claim 7, in particular, Applicant agrees with the Examiner that Schneier does not disclose transmitting the short-term value to the second device prior to or concurrently with producing the secret value. In contrast, Applicant further submits that the last paragraph of page 499 of Menezes §12.3 does not disclose transmitting the short-term value to the second device prior to producing the secret value. Rather, it is directed to a key transport protocol unrelated to the information concerned by the Examiner to be the "short-term value" in claim 1.

In view of the foregoing, Applicant respectfully requests withdrawal of the §103(a) rejection as applied to new claim 7.

With respect to claim 8, Applicant respectfully disagrees that it would have been obvious to apply the teachings of Menezes §10.2 (Handbook of Applied Cryptography," section 10.2) to suggest that the hash operation used to generate the session key may have been done successively. Menezes §10.2 teaches that the session key is determined based on a permutation or keyed one-way hash function, and not an iterative function being performed.

In view of the foregoing, Applicant respectfully requests withdrawal of the §103(a) rejection as applied to claim 8.

Claim 9 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Pitchenik (USP 6,397,328) in view of Menezes (Handbook of Applied Cryptography," section 12.2-12.3 hereinafter referred to as "Menezes §12.2/3"). Applicant respectfully traverses the rejection because neither Pitchenik nor Menezes §12.2/3, alone or in combination, describe or suggest (1) generating a short term value within the first device, the short term value is modified *after each power cycle*, and (2) generating a secret value within the first device *after each power cycle*, the secret value being a combination of both the long term value and the short term value. Emphasis added. Hence, withdrawal of the §103(a) rejection is respectfully requested.

Claims 10-13 are rejected under 35 U.S.C § 103(a) as being unpatentable over Pitchenik in view of Menezes §12.2/3 and Ugon. Applicant traverses the Official Notice in that additional limitations have been added to claim 11. Withdrawal of the §103(a) rejection as applied to claims 10-13 is respectfully requested.

Claim 14 is traversed based on the same agreements regarding lack of teaching for iterative hash functions

Claims 15, 16 and 18 are rejected under 35 U.S.C § 103(a) as being unpatentable over Davis1 (USP 5,818,939) in view of Menezes §12.3 and Burns ("INTEL: Intel introduces new chipset for Intel Pentium III processor-based performance PCs"). Claim 17 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis1 in view of Menezes §12.3, Burns and Davis2 (USP 5,949,881). Claim 19 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis1 in view of Menezes §12.3, Burns, Davis2 and Menezes §10.2. Claim 20, 22-23, 25-26 and 28 are rejected under 35 U.S.C. §103(a) as being unpatentable over Davis1 in view of Menezes §12.3. Claim 21 and 27 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis1 in view of Menezes §12.3 and Ugon. Claim 24 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Davis1 in view of Menezes §12.3 and Menezes §10.2. Applicant respectfully traverses these rejections in their entirety.

Davis1 describes a chipset (315) supporting bulk cryptographic operations. A cryptographic unit (335), separate from the chipset (315), is described as including non-volatile memory (610) for storage of a shared secret key imprinted during manufacture. *See column 5, lines 25-38 of Davis1*. The shared secret key is considered to be the long-term value set forth in claim 15. *See page 10 of the Office Action*. The cryptographic unit further generates a session key. *See column 6, lines 26-28 of Davis1*. The session key is considered to be the short-term value. *See page 10 of the Office Action.*

With respect to the rejection of independent claims 15, 20 and 25, Applicant respectfully disagrees that it would have been obvious to modify the platform set forth in Davis1 per the teachings of Menezes §12.3. The combination of the session key with the symmetric key is not suggested and, in fact, is counter-productive to a system that utilizes both key types. There is no motivation for such combination in order to produce a secret value as claimed. In fact, the key update of Menezes §12.3 appears to be directed to the updating of session keys, namely updating the short-term value.

Applicant respectfully submits that the above-identified rejections of claims 15, 20 and 25 as well as those claims dependent thereon, constitute impermissible hindsight reconstruction. As stated by the Federal Circuit in *In re Kotzab*, 217 F.3d 1365, 55 U.S.P.Q.2d 1313 (Fed. Cir. 2000), "to establish obviousness based on a combination of the elements disclosed in the prior art, *there must be some motivation, suggestion or teaching of the desirability of making the specific combination that was made by the Applicant.*" Emphasis added. Herein, Applicant respectfully submits that none of these references provide motivation for computing the secret value as claimed. Accordingly, Applicant respectfully traverses the grounds for rejection and respectfully requests the Examiner to withdraw the rejections.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: October 27, 2004 By _____

William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: October 27, 2004

FACSIMILE

☒ *transmitted by facsimile to the Patent and Trademark Office.*

Susan McFarlane October 27, 2004
Date